

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No. 2:21-mj-437

The residence located at 1009 Lilley Avenue, Apartment B, ..
Columbus Ohio, 43206 including any person located therein
who may possess any form of digital device, and any digital
devices located therein/thereon

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B, INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 922	Possession of a firearm by a convicted felon
21 U.S.C. 841	Distribution or possession with intent to distribute controlled substances
21 U.S.C. 846	Conspiracy to possess with intent to distribute controlled substances

The application is based on these facts:

SEE ATTACHED AFFIDAVIT, INCORPORATED HEREIN BY REFERENCE

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

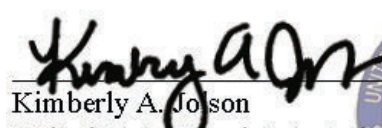
 #2307
Applicant's signature

Jerry Orick, ATF TFO
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/25/2021

City and state: Columbus, Ohio


Kimberly A. Johnson
United States Magistrate Judge



**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION**

**IN THE MATTER OF THE SEARCH OF:
The residence located at 1009 Lilley Ave.
Apartment B, Columbus, Ohio 43206
including curtilage, detached buildings, any
person located therein who may possess any
form of digital device, and any digital devices
located therein/thereon**

Case No. 2:21-mj-437

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Jerry Orick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known 1009 Lilley Ave. Apartment B, Columbus, Ohio 43206, hereinafter "Premises," further described in Attachment A, for the things described in Attachment B.

2. I am a Columbus, Ohio Division of Police (CPD) detective assigned as a Task Force Officer (TFO) with the Alcohol, Tobacco, and Firearms Bureau (ATF). I have been employed by the Columbus Division of Police since 2001. My responsibilities as a Task Force Officer include the investigation of violent criminal street gangs, narcotics and firearms traffickers, money launderers, and firearms-related crimes. I have participated in the execution of search warrants and arrests related to the above-referenced offenses.

3. Through this investigation, investigators have discovered that Willie FELDER, Sr. has a history of criminal activity related to drug trafficking and weapons offenses. More

recent investigations and information, as detailed below, suggest that FELDER is now involved in additional criminal activity related to narcotics trafficking.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. I have not omitted any facts that would negate probable cause.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(g)(1) (possession of a firearm after having been convicted of a crime punishable by more than one year of incarceration) and 21 U.S.C. §§ 841(a)(1) and 846 (possession with intent to distribute controlled substances, and conspiracy to do the same) have been committed by FELDER. There is also probable cause to search the Premises described in Attachment A for evidence, instrumentalities, and/or fruits of these crimes, as further described in Attachment B.

APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code Section 922(g)(1) makes it a federal crime for any person to possess a firearm after having been convicted of a crime punishable by more than one year of incarceration.

7. Title 21 United States Code Section 841 makes it a federal crime for any person to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute or dispense a controlled substance. Subsection (b) of this section specifies that such controlled substances include, among others, cocaine, cocaine base, methamphetamine, heroin, N-phenyl-N-[1-(2-phenylethyl)-4-piperidinyl] propanamide, commonly referred to as fentanyl, and any of

their isomers. Title 21 United States Code Section 846 makes it a crime for any person to attempt or conspire to commit any offense defined in Section 841.

8. The term “computer” is defined in Title 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

9. The terms “records”, documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (such as writings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (such as printing or typing) or electrical, electronic or magnetic form (such as any and all digital data files and printouts or readouts from any magnetic, electrical, or electronic storage device).

BACKGROUND REGARDING ACTIVITIES OF DRUG TRAFFICKERS

10. Your affiant has learned through training and experience the ways in which narcotics traffickers conduct their business, including methods of distributing narcotics, the use of home-based telephones and the use of cellular telephones, and the use of vehicles to facilitate their illegal activities. Your affiant’s training and experience as a CPD detective and an ATF TFO form the basis of the opinions and conclusions set forth below. Based on your affiant’s training, experience, and the experience of other officers, detectives, and agents, your affiant is aware:

- a. that narcotics traffickers often place assets in names other than their own and/or use fictitious identification to avoid detection of these assets by government agencies or local law enforcement;
- b. that even though these assets are in other persons' names the narcotics traffickers continue to exercise dominion and control;
- c. that narcotics traffickers must maintain and finance their ongoing narcotics activities, as well as for paying bills, acquiring assets, and making other purchases;
- d. that it is common for narcotics traffickers to maintain books, records, receipts, notes, ledgers, airline tickets, bus tickets, rental car receipts, receipts relating to the purchase of financial instruments and/or the transfer of funds, and other papers relating to the transportation, ordering, purchasing, processing, storage, sale and distribution of drugs, and the collection of its proceeds. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the narcotics traffickers have ready access to them;
- e. that it is common for narcotics traffickers to conceal contraband, proceeds of drug sales, records of drug transactions, large amounts of currency, financial instruments, precious metals, jewelry, and other items of value; and evidence of financial transactions relating to obtaining, transferring, secreting, and spending large sums of money made from engaging in narcotics trafficking activities in secure locations within their residences and/or other locations over which they maintain dominion and control, in order to have ready access to them;
- f. that it is common for persons involved in narcotics trafficking to maintain evidence pertaining to their obtaining, transfer, concealment, and/or expenditure of narcotic proceeds, such as: currency, financial instruments, precious metals and gem stones, jewelry, books, records, invoices, receipts records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, loan records, money orders, bank drafts, cashier checks, bank checks, wire transfers, safe deposit box keys and money wrappers. These items are maintained by the narcotics traffickers within their residences and/or other locations which they maintain dominion and control;
- g. that when drug traffickers amass a large amount of proceeds from the sale of drugs, the drug traffickers attempt to legitimize these profits;
- h. that to accomplish these goals, narcotics traffickers utilize, including, but not limited to, foreign and domestic banks and their attendant services, Western Union and other wire transfer or Money Service Businesses sales agents, check cashing

services, real estate agents, securities brokers, accountants, attorneys, business fronts, and otherwise legitimate businesses which generate large quantities of currency;

- i. that narcotics traffickers often utilize electronic equipment such as currency counting machines, telephone answering machines, telephone caller identification boxes, and cellular telephones in their drug activities;
- j. that drug traffickers often take or cause to be taken photographs/video tapes of themselves, their associates, their property, and their products. These traffickers usually maintain these photographs/video tapes in their residences and/or other locations in which they maintain dominion or control, including on electronic devices which are used to post such photographs/videos on social media or other websites or applications;
- k. that the sale of controlled dangerous substances, generates large quantities of United States currency (aka, street money);
- l. that is common for drug dealers to separate their “street money” by denomination and put this currency in rubber banded stacks in varying \$1,000 increments to facilitate quick counting;
- m. that the Currency Transaction Report (CTR - IRS Form 4789), which is required to be completed and filed with the Internal Revenue Service by all financial institutions on every currency transaction which exceeds \$10,000, causes tremendous problems for narcotics traffickers when they attempt to negotiate their illegal profits at a financial institution;
- n. that in order to evade the filing of a CTR, narcotics traffickers often “structure” their currency transactions so that no one transaction exceeds \$10,000 or they provide false or misleading information in an attempt to legitimize or conceal the source and/or ownership of the currency;
- o. that narcotics traffickers commonly maintain addresses or telephone numbers in books or papers, which reflect names, addresses and/or telephone numbers of their suppliers, customers, and other associates involved in their narcotics trafficking organization;
- p. that drug traffickers commonly have in their possession, that is on their person, at their residences and/or other locations over which they maintain dominion and control, firearms, including but not limited to: handguns, pistols, revolvers, rifles, shotguns, machine guns, and other weapons. Said firearms are used to protect and

secure a drug trafficker's property. Such property may include, but is not limited to: narcotics, jewelry, narcotics paraphernalia, books, records, and U.S. Currency; and

- q. that courts have recognized unexplained wealth is probative evidence of crimes regarding, in particular, trafficking in narcotics.

INVESTIGATION AND PROBABLE CAUSE

11. On June 17, 2021, a Grand Jury in this District returned a multi-count indictment charging FELDER and two codefendants with violations of, among other statutes, 21 USC 841(a)(1), 21 USC 841(b)(1)(B)(iii), 21 USC 841(b)(1)(C), 21 USC 846, and 18 USC 922(g)(1) and 924(a). The indictment alleges, among other things, that FELDER and multiple codefendants engaged in a narcotics-trafficking conspiracy involving cocaine base (commonly referred to as crack or crack cocaine), fentanyl, methamphetamine, cocaine, and heroin, and that this conspiracy took place from approximately 2018 until approximately October 28, 2020. In addition, your affiant notes the following additional facts that further bear on probable cause regarding this affidavit and application.

A. Willie FELDER, Sr.'s Criminal History

12. In Franklin County, Ohio Common Pleas Case 01CR005266 FELDER was convicted of one count of participating in a criminal gang and ten (10) counts of trafficking in drugs. In Franklin County, Ohio Common Pleas Case 04CR005578 FELDER was convicted of felonious assault and weapons under disability. Both convictions qualify as crimes punishable by more than one year of incarceration.

B. Narcotics Trafficking

13. Willie FELDER, Sr. and his associates have been the targets of an ongoing drug investigation by CPD since approximately February of 2018. Below is a summary of the investigation and relevant facts as it relates to FELDER:

14. FELDER was present at 1190 Lilley when a narcotics SW is executed in February of 2018. On or about February 1, 2018, CPD executed a narcotics search warrant at 1190 Lilley Avenue in Columbus, and FELDER and another individual were present inside the house at the time of the search warrant. The search yielded approximately 15.38 grams of cocaine, as well as an amount of marijuana. Subsequent investigation in 2020 demonstrated that 1190 Lilley was one of FELDER'S primary residences. For example, he slept there and frequented there. Surveillance tied him there. A trash pull tied him there—via his and his girlfriend's name being on a bill. And package found in a subsequent search warrant executed at a house on Ellsworth, detailed below, listed FELDER's name and his 1190 Lilley address. There was also a firearm found at this search. Your affiant further notes that, in 2018 and 2019, law enforcement observed multiple buys by a confidential information ("CI") of small amounts of crack at 1190 Lilley Avenue.

15. FELDER was connected with the circumstances underlying a search warrant that was executed at 896 Ellsworth, Columbus, Ohio on or about February 19, 2020. Multiple individuals tied to FELDER were present at the Ellsworth house. Further connecting FELDER to 896 Ellsworth, one of the phones seized during the search on or about February 19, 2020 was

tied directly to FELDER. On that phone, FELDER indicates via multiple texts, with multiple people, that the house on Ellsworth is his home. FELDER also cites Ellsworth as the place where individuals with whom he was communicating should come to finalize a narcotics transaction. The following items were found on or about February 19, 2020:

- Approximately 90 grams of cocaine
- Approximately 11.6 grams of crack
- Approximately 3.5 grams of fentanyl
- Two firearms
- US Currency

16. FELDER is connected to an additional search warrant executed at 896 Ellsworth in September of 2020. On or about September 16, 2020, FELDER showed up to Ellsworth about 15 minutes before a CPD narcotics search warrant was executed. He was carrying a teal bag as he entered the house. A short time after entering the house, FELDER left the house right before the search was executed. The teal bag was found to have 16.4 grams of a substance containing methamphetamine. Also found were small amounts of fentanyl and cocaine. The search turned up other indicia of drug trafficking, such as scales and magazines, as well as three firearms.

17. FELDER is additionally connected to a search warrant executed at 1009 Lilley Ave., Apartment A Columbus, Ohio executed on or about October 26, 2020. FELDER was present for the search at 1009 Lilley Ave. Apartment A that occurred on or about October 26, 2020, and was subsequently arrested in connection with the search. Investigators listened to a jail call after the search warrant made by FELDER. FELDER made statements admitting that

there was money inside a mattress at 1009 Lilley Ave. Apartment A, and that some of the clothing in the residence belonged to a coconspirator. The following items were found:

- Approximately 20 grams of fentanyl and/or fentanyl analogues
- Approximately 7 grams of crack
- Two firearms
- US Currency

18. FELDER is connected to a search warrant executed at 1414 E. Columbus Apt. C., Columbus, Ohio on or about October 26, 2020. At the time of the search of 1009 Lilley Ave. Apartment A, investigators tracked an individual tied to FELDER who ran from the area near 1009 Lilley Ave. Apartment A to the nearby location of 1414 E. Columbus Apt. C. This individual had an active warrant for possessing a weapon under disability. During the arrest of the individual, law enforcement observed firearms and narcotics in plain view at 1414 E. Columbus Apt. C. Found in a subsequent search of the apartment were the following items, among others:

- Two cell phones, both of which are attributed to one of FELDER's associates
- 4 semi-automatic handguns and AR pistol
- Approximately 38 grams of crack

19. Your affiant is aware that, from the above-described searches, law enforcement seized more than 20 cellular phones and at least one laptop computer. Moreover, multiple of the phones seized were tied directly to FELDER. And multiple such phones contained significant communications related to the trafficking of illegal narcotics. Moreover, the investigation has

not identified that FELDER has any other means of employment beyond the alleged trafficking of illegal narcotics.

20. Continuing up to the present affidavit, during surveillance in May and June of 2021 investigators observed FELDER entering 1009 Lilley Ave on multiple occasions. Investigators also observed several of the vehicles registered to FELDER parked near 1009 Lilley Ave. On or about April 21, 2021 FELDER renewed his Ohio Identification Card. FELDER listed 1009 Lilley Ave Apt B, the Premises, as his residence.

21. On or about June 1, 2021, during surveillance investigators observed suspected narcotics activity taking place on the rear second floor of 1009 Lilley Ave. The suspected narcotics activity included multiple short stop-and-meet transactions in or around the Premises. Based upon training and experience, law enforcement has reason to believe that such conduct was consistent with narcotics trafficking. FELDER was observed going up and coming down the rear stairs of 1009 Lilley Ave at the time of or near the time of these suspected narcotics transactions.

22. On or about June 3, 2021, during surveillance investigators observed suspected narcotics activity at 1009 Lilley Ave. The suspected narcotics activity included multiple short stop-and-meet transactions in or around the Premises. Based upon training and experience, law enforcement has reason to believe that such conduct was consistent with narcotics trafficking. Vehicles registered to FELDER were observed parked near 1009 Lilley Ave.

23. As stated above, on June 17, 2021, a Grand Jury in this District returned a multi-count indictment charging FELDER and two codefendants with violations of, among other

statutes, 21 USC 841(a)(1), 21 USC 841(b)(1)(B)(iii), 21 USC 841(b)(1)(C), 21 USC 846, and 18 USC 922(g)(1) and 924(a).

24. On or about June 25, 2021, members of the United States Marshals Service (USMS) conducted surveillance on 1009 Lilley Avenue, Apartment B, Columbus, Ohio in preparation of FELDER's arrest pursuant to the arrest warrant issued regarding the above-described indictment. Upon approach, USMS members observed an individual later identified as Willie FELDER look out the window of 1009 Lilley Ave., Apt B., Columbus, Ohio. FELDER was instructed to open the door of the apartment. FELDER opened the door. While this was occurring, a male exited the rear of 1009 Lilley Ave., Apt B., Columbus, Ohio. This male was detained as he exited the property in order to check his identity and ensure officer safety. He identified himself as Johnny Blackwell. It was determined that this was a false name, and the male was positively identified as Ravon Ingram. Ingram was found to have several felony warrants for his arrest. Law enforcement further determined that Ingram has a felony conviction for felonious assault from Franklin County Common Pleas case 06CR002920. This conviction would prohibit Ingram from possession of a firearm. While taking FELDER into custody, suspected marijuana and drug paraphernalia were observed in plain view. One other individual was detained inside of the residence. Two empty holsters were observed—one on top of a purse and one on a bed-side table. The other person found inside the home was identified as Seqoyia Jackson, an individual law enforcement knows based upon prior investigation to be closely associated with FELDER. Jackson was asked about the holsters and if there were firearms for the

holsters. JACKSON stated that there were firearms in home and stated that the firearms could be in a few different locations.

TECHNICAL TERMS

25. Based on my training and experience, I use the following technical terms to convey the following meanings:
- a. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
 - b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
 - c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

26. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

27. *Probable cause.* In addition to the facts provided above, I submit that if a computer or storage medium is found on the Premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

28. Based upon training, knowledge, and experience, I am aware that computer equipment is often used by narcotics traffickers to generate, store, and/or print documents used in narcotics-trafficking schemes. Similarly, your affiant is aware that FELDER utilized cellular

phones to communicate with customers who purchased narcotics from him. As such, there is reason to believe that there are computer system(s) and/or other digital devices currently located on the Premises that relate to the crimes for which FELDER and his coconspirators have been indicted.

29. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and

malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves.

- Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

30. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a Premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the Premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on Premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or

knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.


CONCLUSION

32. I submit that this affidavit supports probable cause for a warrant to search the Premises described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,


Jerry Orick
Task Force Officer, ATF

Subscribed and sworn to before me this ^{25th} ___ day of June, 2021.


Kimberly A. Johnson
United States Magistrate Judge



ATTACHMENT A
Property to be searched

The place to be searched is the residence described below, in particular 1009 Lilley Ave. Apartment B, which includes all its appurtenances, parking areas, outdoor working areas, detached buildings tied to Apartment B, as well as individuals at the residence who may be in possession of a mobile computing device, including cellular telephones and laptops, and any computing-related devices or digital media located therein or thereon.

The place to be searched is further described as 1009 Lilley Ave. Apartment B, Columbus, Ohio 43206, a two-story, multi-unit apartment building. A photo of the exterior of the apartment building in which Apartment B is located is attached below:



ATTACHMENT B
Property to be seized

1. All records relating to violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute a controlled substance) those violations involving Willie FELDER, including:
 - a. Books, records, notes, ledgers, and other papers relating to the transportation, purchase, distribution, packaging, and sale of controlled substances, which books, records, notes, ledgers, and other papers may be maintained in either paper form or on computers;
 - b. Cash, currency, jewelry, currency counters, financial instruments, and records relating to controlled substances, expenditure of proceeds of drug transactions, fraud, and evidence of financial transactions relating to obtaining, transferring, concealing, or spending of large sums of money made from engaging in drug trafficking;
 - c. Bank and other financial institution records consisting of savings, loans, records of deposits, statements, letters of credit, money orders, cashier checks, passbooks, cancelled checks, certificates of deposit, lease agreements, customer account information, income and expense summaries, cash disbursement journals, financial statements, state and federal income tax returns, information related to the receipt and other disposition of income, and related financial information pertaining to the purchase, lease, sale or other disposition of real or personal property, including real estate, automobiles, jewelry, and furniture;

- d. Proof of residency, including but not limited to cancelled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents and keys;
 - e. Safe deposit box lease agreements and safe deposit keys;
 - f. Any safes, vaults, or secured storage equipment that could secret any of the above listed items, and the contents therein, with the ability to open by force if necessary;
 2. Firearms, firearm parts, and accessories.
 3. Illicit narcotics and narcotics trafficking paraphernalia to include scales, blenders, and narcotics packaging material.
 4. Computers or storage media used as a means to commit the violations described above or store information related to the violations described above.
 5. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence

of the presence or absence of security software designed to detect malicious software;

- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.